HOW I LEARNED TO STOP WORRYING AND DISMANTLE THE BOMB
NEW APPROACHES TO NUCLEAR WARHEAD VERIFICATION

Alex Glaser,* Sébastien Philippe,* and Robert J. Goldston**

*Princeton University
**Princeton University and Princeton Plasma Physics Laboratory

Duke University, January 19, 2017
Five-year project, funded by U.S. DOE, 13 U.S. universities and 9 national labs, led by U-MICH

Princeton participates in the research thrust on disarmament research
(and leads the research thrust of the consortium on policy)
INTERNATIONAL PARTNERSHIP
FOR NUCLEAR DISARMAMENT VERIFICATION

Established in 2015; currently 26 participating countries

Working Group One: “Monitoring and Verification Objectives” (chaired by Italy and the Netherlands)
Working Group Two: “On-Site Inspections” (chaired by Australia and Poland)
Working Group Three: “Technical Challenges and Solutions” (chaired by Sweden and the United States)

www.state.gov/t/avc/ipndv
WHAT’S NEXT FOR NUCLEAR ARMS CONTROL?

2015 STATEMENT BY JAMES MATTIS

“The nuclear stockpile must be tended to and fundamental questions must be asked and answered:

• We must clearly establish the role of our nuclear weapons: do they serve solely to deter nuclear war? If so we should say so, and the resulting clarity will help to determine the number we need.
• Is it time to reduce the Triad to a Diad, removing the land-based missiles? This would reduce the false alarm danger.
• Could we re–energize the arms control effort by only counting warheads vice launchers?
• Was the Russian test violating the INF treaty simply a blunder or a change in policy, and what is our appropriate response?”

General James N. Mattis, USMC (Ret.)
Former Commander, United States Central Command

Senate Armed Services Committee
Global Challenges and U.S. National Security Strategy
January 27, 2015
WHAT IS TO BE VERIFIED?
WHAT IS TO BE VERIFIED?

SELECTED CURRENT AND EMERGING VERIFICATION CHALLENGES FOR NUCLEAR ARMS CONTROL AND NONPROLIFERATION

1. VERIFYING NUMERICAL LIMITS OF DECLARED NUCLEAR WARHEADS

Requires techniques to account for (and identify) nuclear warheads in storage for example, using (hashed) declarations, special tags, and/or unique identifiers (UIDs)

2. CONFIRMING THE AUTHENTICITY OF NUCLEAR WARHEADS

Requires dedicated inspection systems for example, based on radiation-detection techniques (passive/active, neutron/gamma)

3. ESTABLISHING CONFIDENCE IN THE ABSENCE OF UNDECLARED STOCKS OR PRODUCTION

How to make sure that no covert warheads/materials exist outside the verification regime?
No silver bullet; but not much different from existing NPT verification challenges

Source: Paul Shambroom (top), Google Earth (middle), and U.S. Department of Energy (bottom)
THOUSANDS OF NUCLEAR WEAPONS ARE CURRENTLY NON-DEPLOYED (i.e., IN RESERVE OR AWAITING DISMANTLEMENT)

W87/Mk-21 Reentry Vehicles in storage, Warren Air Force Base, Cheyenne, Wyoming

Photo courtesy of Paul Shambroom, www.paulshambroom.com
NUCLEAR WARHEAD VERIFICATION

KEY CONCEPTS OF (PROPOSED) SYSTEMS

ATTRIBUTE APPROACH
Confirming selected characteristics of an object in classified form (for example, the presence/mass of plutonium)

TEMPLATE APPROACH
Comparing the radiation signature from the inspected item with a reference item ("golden warhead") of the same type

INFORMATION BARRIERS
Technologies and procedures that prevent the release of sensitive nuclear information (generally needed for both approaches)

edited by D. Spears, 2001
PREVENTING THE EXCHANGE OF SENSITIVE INFORMATION DURING A RADIATION MEASUREMENT

**Trusted Information Barrier**

- Measure (but sanitize) sensitive information
- “Hard” to authenticate and certify
- Single-bit observation

**Interactive Zero-knowledge Proof**

- Never measure sensitive information
- “Easy” to authenticate and certify
- More complex observation


56th Annual INMM Meeting, July 12-16, 2015, Indian Wells, California
PREVENTING THE EXCHANGE OF SENSITIVE INFORMATION DURING A RADIATION MEASUREMENT

**Trusted Information Barrier**

Measure (but sanitize) sensitive information

“Hard” to authenticate and certify

Single-bit observation

**Interactive Zero-knowledge Proof**

Never measure sensitive information

“Easy” to authenticate and certify

More complex observation


56th Annual INMM Meeting, July 12-16, 2015, Indian Wells, California
INTERACTIVE ZERO-KNOWLEDGE PROOFS

LOGICAL LAYER
Zero-Knowledge Proofs: The prover (P) convinces the verifier (V) that s/he knows a secret without giving anything about the secret itself away.


Graphics adapted from O. Goldreich, *Foundations of Cryptography*, Cambridge University Press, 2001; and eightbit.me
EXAMPLE

FOR AN “ILLUSTRATED PRIMER” ON ZERO-KNOWLEDGE PROOFS, SEE
blog.cryptographyengineering.com/2014/11/zero-knowledge-proofs-illustrated-primer.html

FOR A ZERO-KNOWLEDGE “SUDOKU” PROOF, SEE
www.wisdom.weizmann.ac.il/~naor/PAPERS/SUDOKU_DEMO/
PROVING THAT TWO OBJECTS ARE IDENTICAL

“THE DAY BEFORE THE INSPECTION”

1. Alice owns valuable objects whose design she wants to keep a secret
2. In private, she takes a radiograph of this object on “blank film”
3. Alice prepares two identical complements of that picture and places these complements in two sealed envelopes
PROVING THAT TWO OBJECTS ARE IDENTICAL

“THE DAY OF THE INSPECTION”

(4) At the day of the inspection, Alice presents a reference item and an item for inspection in concealed form
(5) Bob randomly assigns the envelopes; then, new radiographs of both items are made
(6) If Alice presents a valid item, a “flat image” is produced; if not, she risks failing the inspection (and revealing information)
PROVING THAT TWO OBJECTS ARE IDENTICAL

“THE DAY OF THE INSPECTION”

(4) At the day of the inspection, Alice presents a reference item and an item for inspection in concealed form.

(5) Bob randomly assigns the envelopes; then, new radiographs of both items are made.

(6) If Alice presents a valid item, a “flat image” is produced; if not, she risks failing the inspection (and revealing information).
PROVING THAT TWO OBJECTS ARE IDENTICAL

"THE DAY OF THE INSPECTION"

We will later introduce the maximum possible exposure as \( N_{\text{MAX}} \)
WHAT THE PROTOCOL ACHIEVES

**COMPLETENESS**

If the items are identical and both host and inspector follow the protocol, then the inspector will accept with probability $p = 1 - (\frac{1}{2})^n$

**SOUNDNESS**

If the items are different and the inspector follows the protocol, then, no matter what the host does, the inspector will reject with probability $p \geq 1 - (\frac{1}{2})^n$

**ZERO KNOWLEDGE**

As long as the host follows the protocol and presents matching items, the inspector gains no knowledge during their interaction except for the fact that the items match.


*56th Annual INMM Meeting*, July 12-16, 2015, Indian Wells, California
PHYSICAL ZERO-KNOWLEDGE PROOFS
WITH NON-ELECTRONIC PRELOADABLE DETECTORS

THIS BASIC IDEA HAS TRIGGERED INTEREST IN OTHER “PHYSICAL APPLICATIONS” OF ZERO-KNOWLEDGE
see, for example, B. Fisch, D. Freund, M. Naor, “Physical Zero-Knowledge Proofs of Physical Properties”
14 MeV neutron generator
*(Thermo Scientific P 385)*

Collimator slot

Test object

Collimator

Detector array
SUPERHEATED DROPLET DETECTORS OFFER A WAY TO IMPLEMENT THIS PROTOCOL AND AVOID DETECTOR-SIDE ELECTRONICS

Superheated C-318 fluorocarbon (C₄F₈) droplets suspended in aqueous gel
Tailor-made by d’Errico Research Group, Yale University
Sensitive to neutrons with Eₙ > Eₘᵦ
Designed to be insensitive to γ-radiation

Active volume ........... : 6.0 cm³
Droplet density ........... : 3500 cm⁻³
Droplet diameter ...... : ~100 µm
Absolute Efficiency ... : 4 x 10⁻⁴
FLUENCE RESPONSE

OF SUPERHEATED EMULSIONS MEASURED AS A FUNCTION OF NEUTRON ENERGY AND TEMPERATURE

Francesco d’Errico, “Radiation Dosimetry and Spectrometry with Superheated Emulsions”
SUPERHEATED DROPLET DETECTORS

BUBBLES CAN BE COUNTED WITH A VARIETY OF TECHNIQUES

Detectors can be “reset” (bubbles recompressed) many times (good for R&D)
Inspector can verify functionality of detectors after inspection

Optical readout (with camera)
Source: Bubble Technologies Industries

Volumetric readout

Opto-electronic readout
Adapted from: Francesco d’Errico, Yale

Photodiodes collecting light scattered by bubbles
Diode output scales (quasi) linearly with bubble count

LEDs
RESULTS

RADIOGRAPHY WITH 14-MeV NEUTRONS
(SIMULATED DATA)
ZERO-KNOWLEDGE VERIFICATION

RADIOGRAPHY WITH 14 MeV NEUTRONS

Simulated data from MCNP calculations; neutron detection energies > 10 MeV; N(max) = 5,000
ZERO-KNOWLEDGE VERIFICATION

RADIOGRAPHY WITH 14 MeV NEUTRONS

Simulated data from MCNP calculations; neutron detection energies > 10 MeV; N(max) = 5,000
ZERO-KNOWLEDGE VERIFICATION

LOCAL TUNGSTEN DIVERSION (540 GRAMS)

543 grams of tungsten removed from outer ring of test object; simulated data from MCNP calculations; neutron detection energies > 10 MeV

EXPERIMENTAL RESULTS

The Conjurer, Hieronymus Bosch, 1502
EXPERIMENTAL SETUP AND SCENARIO

WE WISH TO IDENTIFY CASES IN WHICH THE CUBE PATTERN HAS BEEN ALTERED WITHOUT GAINING ANY INFORMATION ABOUT THE CONFIGURATION IN CASES WHERE IT HAS NOT

Collimated neutron beam
14-MeV (DT) generator

Reference item consists of a combination of 2-inch cubes (aluminum and stainless steel)

Reference item

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td>AL</td>
<td>SS</td>
</tr>
<tr>
<td>AL</td>
<td>AL</td>
<td>SS</td>
</tr>
</tbody>
</table>

Detector positions

1 2 3 4 5 6 7

Detector array

Staging area
(with reference item)
EXPERIMENTAL RESULTS

(VALID ITEM)

Reference item

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>X</td>
<td>AL</td>
<td>SS</td>
</tr>
<tr>
<td>AL</td>
<td>AL</td>
<td>SS</td>
</tr>
</tbody>
</table>

Bubble count

N_{\text{MAX}} = 1020

EXPERIMENTAL RESULTS

(A DRASTIC CHANGE)

Reference item

```
X  X  X
X  AL SS
AL AL SS
```

"Mirrored item"

```
X  X  X
SS AL X
SS AL AL
```

Bubble count

- N_{MAX} = 1020

WHAT'S NEXT?
FISSION CROSS SECTIONS
OF THE MAIN URANIUM AND PLUTONIUM ISOTOPES

Rob’s Idea:
Let’s interrogate with neutrons in the 300-keV range and look for fission neutrons (> 1 MeV)

Source: Evaluated Nuclear Data File (ENDF), www-nds.iaea.org/exfor/endf.htm
“TWO-COLOR INTERROGATION”
INTERROGATION WITH NEUTRONS FROM (p-\textsuperscript{7}Li) REACTION
(tuned to \(~300\) keV energy cutoff)
TOTAL NEUTRON YIELD CURVES FOR SELECTED (THRESHOLD) REACTIONS

David L. Chichester, *Production and Applications of Neutrons Using Particle Accelerators*
INL/EXT-09-17312, Idaho National Laboratory, November 2009
SIMULATED p-Li NEUTRON SOURCE

SPECTRUM CAN BE TAILORED BY ADJUSTING THE INCIDENT PROTON ENERGY AND THE THICKNESS OF THE LITHIUM TARGET

Source: SIMLiT simulations by Yan Jie, Princeton University
BARE PLUTONIUM SPHERE

8.00 cm DIAMETER SPHERE, WEAPON-GRADE PLUTONIUM

Test item based on BeRP ball, see J. Mattingly and D. J. Mitchell, *Applied Radiation and Isotopes*, 70 (2012), 1136–1140

**“Radiograph”**
(never measured)

Essentially no structure in data, but absolute values secret
Here: ~1,540 bubbles average
(unknown to inspector)

**Valid item**

Simulated data from MCNP6 calculations, neutron detection energies > 500 keV
N(max) = 10,000, i.e., 6–7 times higher than actual values from test item

**Invalid item**

(Isotopic shift from 93.7% to 81.2% Pu-239)
BARE PLUTONIUM SPHERE

8.00 cm DIAMETER SPHERE, WEAPON-GRADE PLUTONIUM

Test item based on BeRP ball, see J. Mattingly and D. J. Mitchell, *Applied Radiation and Isotopes*, 70 (2012), 1136–1140
A TWO-COLOR SETUP AT TUNL?

USING 2 MEV PROTONS FROM TANDEM ON LIF TARGET

6 µA beam
2.04 MeV p⁺

~10²⁸ n/s

~10 µm LiF foil

20 cm

SS SS SS
LEU LEU LEU
SS SS SS

Three 2” cubes
19.75% enriched U
7.5 kg total U
CONCLUSION AND OUTLOOK

**“ONE-COLOR” SETUP**

Neutron transmission radiography using high-energy (14 MeV) neutrons is effective in detecting geometric and elemental differences.

Distinguishing isotopic differences can be more challenging because relevant 14-MeV total and fission cross sections can be similar for some important elements (esp. for Pu-239 vs Pu-240).

**“TWO-COLOR” SETUP**

Fission signatures triggered by ~ 300-keV neutrons are extremely sensitive to isotopic differences (and also to differences in geometry).

Combine with 14-MeV transmission radiography.

Needed for experimental demonstration: Intense 2-MeV proton source.
ACKNOWLEDGEMENTS

PRINCETON AND PPPL

Andrew Carpe
Charles Gentile
Robert J. Goldston
Sébastien Philippe
Yan Jie

ELSEWHERE

Boaz Barak, Microsoft Research New England / Harvard University
Francesco d'Errico, Yale University
Margarita Gattas-Sethi, Yale University

RESEARCH SUPPORTED BY

Global Zero
MacArthur Foundation
Carnegie Corporation of New York
U.S. Department of State
National Nuclear Security Administration, U.S. Department of Energy